(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
19 June 2003 (19.06.2003)

PCT

(10) International Publication Number
WO 03/050784 A1

(51) International Patent Classification[7]: G09C 1/00

(21) International Application Number: PCT/KR02/00695

(22) International Filing Date: 17 April 2002 (17.04.2002)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
2001/78588 12 December 2001 (12.12.2001) KR

(71) Applicant *(for all designated States except US)*: **ELECTRONICS AND TELECOMMUNICATIONS RESEARCH INSTITUTE** [KR/KR]; 161 Kajong-Dong, Yusong-Gu, 305-350 Taejon (KR).

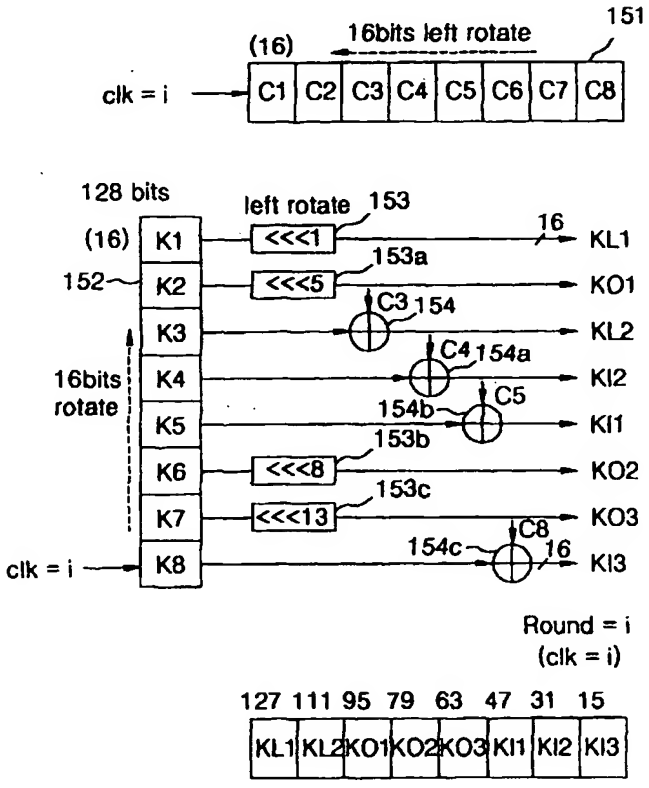
(72) Inventors; and
(75) Inventors/Applicants *(for US only)*: **KIM, Ho Won** [KR/KR]; 236-1 Kajong-Dong, Yusong-Gu, 305-350 Taejon (KR). **CHOI, Yong Je** [KR/KR]; 1216-7 Yongbong-Dong, Book-Gu, 500-070 Kwangju (KR). **RYU, Heui Su** [KR/KR]; 103-801 Sejong Apt., Jeonmin-Dong, Yusong-Gu, 305-728 Taejon (KR). **KIM, Moo Seop** [KR/KR]; 104-504 Sangroksoo Apt., Mannyun-Dong, Seo-Gu, 302-150 Taejon (KR). **HONG, Do Won** [KR/KR]; 510-803 Expo Apt., Jeonmin-Dong, Yusong-Gu, 305-762 Taejon (KR). **CHUNG, Kyo Il** [KR/KR]; 107-1102 Hanwool Apt., Shinsung-Dong, Yusong-Gu, 305-707 Taejon (KR). **PARK, Young Soo** [KR/KR]; 101-907 Sanho-Apt., Tanbang-Dong, Seo-Gu, 302-766 Taejon (KR).

(74) Agent: **LEE, Hwa-Ik**; Young International Patent & Law Firm, 4th Fl. Yosam Bldg., 648-23 Yoksam-dong, Kangnam-gu, Seoul 135-748 (KR).

(81) Designated States *(national)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU,

[Continued on next page]

(54) Title: ENCRYPTION APPARATUS APPLYING KASUMI ENCRYPTION ALGORITHM



(57) Abstract: Disclosed is an encryption apparatus applying a KASUMI encryption algorithm. In the encryption apparatus, a round circuit is constructed through combination of an FL block with an FO block. The FL and FO blocks separate a secret key defined in the KASUMI encryption algorithm and provided from a secret key scheduler and 64-bit text data into 32-bit data, respectively, and perform specified encryption operation functions. The FO block is constructed through a multistage pipeline using a plurality of pipeline registers. The encryption apparatus has a low power consumption, and is small-sized in comparison to the conventional encryption apparatus using the MISTY or DES encryption algorithm. Also, the encryption apparatus can be applied to portable terminals and high-performance servers that require the low power consumption and the small size.

WO 03/050784 A1

CZ, DE, DK, DM, DZ, EC, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, OM, PH, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VN, YU, ZA, ZM, ZW.

(84) Designated States *(regional)*: ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Published:
— *with international search report*

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

ENCRYPTION APPARATUS APPLYING KASUMI ENCRYPTION ALGORITHM

Technical Field

The present invention relates generally to an encryption apparatus, and more particularly to an encryption apparatus applying a KASUMI encryption algorithm.

Background Art

Recently, with the development of the wired and radio communication techniques, the protection of information on networks becomes a matter of increasing concern. Especially, in developing the 3rd generation partnership project (3GPP) system that is the 3rd generation radio communication system, the diverse security characteristics that can protect the information, development of encryption algorithms for authenticating the stability and reliability of the system, and worldwide applicable standardization of techniques are now required.

Accordingly, TSG-SA that is the technical group of the 3GPP system and organized around the standard technique development organizations including European Telecommunications Standards Institute (ETSI) requested SAGE that is the encryption algorithm experts group of ETSI to develop 11 security-related algorithms called f0-f10. The 11 security-related algorithms have been defined in the TS33.102v3.7.0 standard documents.

In the standard documents defining the 11 security-related algorithms developed by SAGE of ETSI as described above, the authentication part defines f1 that is an algorithm for random number generation, an f1 algorithm for subscriber's network authentication, f1* algorithm for resynchronized message authentication, f2 algorithm for subscriber authentication, f3 algorithm for radio-area encryption key generation, f4 algorithm for radio-area integrity key generation, f5 algorithm for subscriber anonymity key generation, and f5* algorithm for resynchronized anonymity key generation. The authentication part also defines an f8 algorithm for radio-area user data encryption required in a terminal and a radio network controller, and f9 that is a radio-area user traffic integrity authentication algorithm.

Especially, after the standardization of the f8 encryption algorithm and the f9 integrity algorithm, a KASUMI encryption algorithm has been newly developed

based on the MISTY that is a secret key encryption algorithm developed and made public by Mitsubishi Corporation in Japan.

However, since the conventional implementation technique applying the KASUMI algorithm in the 3GPP system mostly processes the traffic by software, its throughput is lowered, and a large amount of traffic causes the system to have a large amount of load. For example, the RNC switch equipment of the 3GPP system performs the KASUMI encryption algorithm using a power PC processor, and this causes the system to bear a large amount of load, resulting in that the power PC processor should be additionally used to cause a heavy manufacturing cost and inefficiency.

In the 3GPP system, there are not so many conventional hardwired techniques using the KASUMI encryption algorithm, and thus encryption apparatuses that apply the conventional MISTY encryption algorithm or a data encryption standard (DES) encryption algorithm have been developed.

Especially, Japanese Patent Laid-open Nos. Pyung 09-0269727 "Encryption method and apparatus", Pyung 09-0251267 "Encryption method and apparatus", etc., have been disclosed as the conventional encryption apparatuses applying the DES encryption algorithm. However, since they construct a round circuit in a manner that the round circuit is pipelined through insertion of a register between rounds, the power consumption is severe, and the area required for the apparatus becomes large. This causes the diverse encryption techniques not to be applied to portable terminals or high-performance servers that require the low power consumption and the small installation area.

Disclosure of the Invention

Therefore, an object of the present invention is to solve the problems involved in the prior art and to provide an encryption apparatus applying a KASUMI encryption algorithm wherein a round circuit is constructed through combination of an FL block with an FO block which separate a secret key defined in the KASUMI encryption algorithm and provided from a secret key scheduler and 64-bit text data into 32-bit data, respectively, and perform a specified encryption operation function, and the FO block is constructed through a multistage pipeline using a plurality of pipeline registers.

In order to accomplish the above-mentioned object, the present invention provides an encryption apparatus applying a KASUMI encryption algorithm

comprising a register section for selecting and storing either of text data and input data obtained after performing a round operation, a secret key scheduler for generating secret keys for encrypting the text data, an FL block for operating output data of the register section and the secret key with an FL function defined in the KASUMI encryption algorithm, an FO block for operating the output data of the register section and the secret key with an FI function defined in the KASUMI encryption algorithm and an exclusive-OR function, an adder section for exclusive-OR-gating output data of the FL block and the FO block and the output data of the register section and applying exclusive-OR-gated data to the register section, and an input/output control section for selecting the input data of the FL block and the FO block and selecting paths of the output data of the FL block and the FO block.

In another aspect of the present invention, there is provided an encryption apparatus applying a KASUMI encryption algorithm comprising a pipeline register section for selecting and storing either of text data and input data obtained after performing a round operation, a secret key scheduler for generating secret keys for encrypting the text data, an FL1 block for operating output data of the pipeline register section and the secret key with an FL function defined in the KASUMI encryption algorithm, an FO block having a three-stage pipeline structure and operating output data of the FL1 block and the pipeline register section and the secret key with an FI function defined in the KASUMI encryption algorithm and an exclusive-OR function, FL2 block for operating output data of the FO block and the secret key with the FL function defined in the KASUMI encryption algorithm, an adder section for exclusive-OR-gating output data of the FO block and the FL2 block and the output data of the pipeline register section so that the output data of the FO block and the FL2 block are synchronized with the output data of the pipeline register section and applying exclusive-OR-gated data to the pipeline register section, and an input/output control section for selecting the input data of the FO block and selecting a path of the output data of the FO block.

Brief Description of the Drawings

The above object, other features and advantages of the present invention will become more apparent by describing the preferred embodiments thereof with reference to the accompanying drawings, in which:

FIG. 1 is a view illustrating the construction of an encryption apparatus according to a first embodiment of the present invention.

FIG. 2 is a view illustrating the construction of a secret key scheduler of FIG. 1.

FIG. 3 is a view illustrating the construction of an encryption apparatus according to a second embodiment of the present invention.

FIG. 4 is a view illustrating the construction of an FO block of FIG. 3.

FIG. 5 is a view illustrating the construction of an FI sub-block illustrated in FIG. 4.

FIG. 6 is a view illustrating the construction of another FO block of FIG. 3.

FIG. 7 is a view illustrating the construction of a secret key scheduler of FIG. 3.

FIG. 8 is a view illustrating the construction of another secret key scheduler of FIG. 3.

FIG. 9 is a view illustrating the construction of a two-round circuit implementing the encryption apparatus according to the first embodiment of the present invention.

FIG. 10 is a view illustrating the construction of a two-round circuit for applying a two-stage pipeline which implements the encryption apparatus according to the first embodiment of the present invention.

FIG. 11 is a view illustrating the construction of a two-round circuit for applying a four-stage pipeline that combines the encryption apparatuses according to the first and second embodiments of the present invention.

FIG. 12 is a view illustrating the construction of a two-round circuit for applying an eight-stage pipeline that combines the encryption apparatuses according to the first and second embodiments of the present invention.

Best Mode for Carrying Out the Invention

Now, the encryption apparatus applying a KASUMI encryption algorithm according to preferred embodiments of the present invention will be described in detail with reference to the annexed drawings.

FIG. 1 is a view illustrating the construction of an encryption apparatus according to a first embodiment of the present invention.

Referring to FIG. 1, a first multiplexer 110 of a register section 100 selects and outputs either of upper 32-bit input data of 64-bit text data and 32-bit input data obtained after performing an even round operation.

A first register 120 temporarily stores output data of the first multiplexer 110.

A second multiplexer 130 selects and outputs either of lower 32-bit input data of the 64-bit text data and 32-bit input data obtained after performing an odd round operation.

A second register 140 temporarily stores output data of the second multiplexer 130.

A secret key scheduler 150 generates secret keys for encrypting the 64-bit text data.

An FL block 160 operates output data of the first register 120 and the second register 140 and the secret key Ki from the secret key scheduler 150 with an FL function defined in the KASUMI encryption algorithm, and outputs 32-bit resultant data.

An FO block 170 operates the output data of the first register 120 and the second register 140 and the secret key Ki from the secret key scheduler 150 with an FI function defined in the KASUMI encryption algorithm and an exclusive-OR function, and outputs 32-bit resultant data.

A first adder 180 of an adder section 180A exclusive-OR-gates the even-round 32-bit output data of the FL block 160 and the output data of the first register 120, and outputs the even-round 32-bit data to the first multiplexer 110.

A second adder 190 exclusive-OR-gates the odd-round 32-bit output data of the FO block 170 and the output data of the second register 140, and outputs the odd-round 32-bit data to the second multiplexer 130.

A third multiplexer 200 of an input/output control section 200A applies the output data of the first register 120 to the FL block 160 in the odd round, and applies the output data of the FO block 170 to the FL block 160 in the even round.

A fourth multiplexer 210 applies the output data of the FL block 160 to the FO block 170 in the odd round, and applies the output data of the second register 140 to the FO block 170 in the even round.

A fifth multiplexer 220 applies the output data of the FL block 160 to the fourth multiplexer 210 in the odd round, and applies the output data of the FL block 160 to the first adder 180 in the even round.

A sixth multiplexer 230 applies the output data of the FO block 170 to a second adder 190 in the odd round, and applies the output data of the FO block 170 to the third multiplexer 200 in the even round.

Referring to FIG. 2, a C-constant register 151 of the secret key scheduler 150 stores 8 C-constant values of 16 bits C1, C2, C3, C4, C5, C6, C7, and C8 defined for key scheduling in the KASUMI encryption algorithm, and whenever one clock is generated, one C-constant value rotates to the left side.

A secret key register 152 of the secret key scheduler 150 stores 8 secret key values of 16 bits K1, K2, K3, K4, K5, K6, K7, and K8 defined by a user, and whenever one clock is generated, one secret key value rotates.

The time for the rotation of one secret key value is synchronized with the time for the rotation of one C-constant value to the left side.

A plurality of rotators 153, 153a, 153b, and 153c of the secret key scheduler 150 generate specified secret keys by rotating the specified secret key values of the secret key register 152 to the left side as many as the determined number of bits, respectively.

At an initial state, the four rotators 153, 153a, 153b, and 153c as shown in FIG. 2 generate the secret keys KL1, KO1, KO2, and KO3 by rotating the initial secret key values K1, K2, K6, and K7 stored in the secret key register 152 to the left side by 1 bit, 5 bits, 8 bits, and 13 bits, respectively. Thereafter, they depend on the operation principle of the secret key register 152.

A plurality of adders 154, 154a, 154b, and 154c of the secret key scheduler 150 generate the secret keys by exclusive-OR-gating the specified secret key values of the secret key register 152 and the corresponding C-constant values, respectively.

At an initial state, the four adders 154, 154a, 154b, and 154c as shown in FIG. 2 generate the secret keys KL2, KI2, KI1, and KI3 by exclusive-OR-gating the initial secret key values K3, K4, K5, and K8 stored in the secret key register 152 and the corresponding C-constant values C3, C4, C5, and C8, respectively. Thereafter, the operation of the moving key values and constant values is performed according to the operation of the secret key register 152 and the C-constant register 151.

The encryption apparatus applying the KASUMI encryption algorithm as constructed above according to the present invention operates as follows.

The encryption apparatus illustrated in FIG. 1 includes a low power consumption type round circuit that does not apply the pipeline, and the secret key scheduler 150.A one-round operation is performed for one clock cycle, and the encryption apparatus encrypts the 64-bit text input data by repeatedly performing the round operation eight times in all.

Initially, the upper 32-bit data of the 64-bit text input data is inputted to the first multiplexer 110 through an initial input port 111, and simultaneously the lower 32-bit data of the 64-bit text input data is inputted to the second multiplexer 130 through an initial input port 131.

At this time, the upper 32-bit data inputted to the first multiplexer 110 is stored in the first register via the first multiplexer 110 as indicated as a solid line in FIG. 1. Also, the upper 32-bit data sequentially passes through the third multiplexer 200, FL block 160, fifth demultiplexer 220, fourth multiplexer 210, FO block 170, and sixth demultiplexer 230, and then exclusive-OR-gated with the lower 32-bit data stored in the second register 140 by the second adder 190. The exclusive-OR-gated data is then inputted to an odd-round performing result data input port 132 of the second multiplexer 130.

The 32-bit data exclusive-OR-gated by the second adder 190 and inputted to the second multiplexer 130 is newly stored in the second register 140 via the second multiplexer 130.

The upper 32-bit data newly stored in the second register 140, as shown as a dotted line in FIG. 1, sequentially passes through the fourth multiplexer 210, FO block 170, sixth demultiplexer 230, third multiplexer 200, FL block 160, and fifth demultiplexer 220, and then exclusive-OR-gated with the upper 32-bit data stored in the first register 120 by the first adder 180. The exclusive-OR-gated data is then inputted to an even-round performing result data input port 112 of the first multiplexer 110.

The 32-bit data exclusive-OR-gated by the first adder 180 and inputted to the first multiplexer 110 is newly stored in the first register 120 via the first multiplexer 120.

FIG. 3 is a view illustrating the construction of an encryption apparatus according to a second embodiment of the present invention.

Referring to FIG. 3, a first multiplexer 110a of a pipeline register section 100A selects and outputs either of upper 32-bit input data of 64-bit text data and 32-bit input data obtained after performing an even round operation.

A first pipeline register 120a temporarily stores output data of the first multiplexer 110a.

A second multiplexer 130a selects and outputs either of lower 32-bit input data of the 64-bit text data and 32-bit input data obtained after performing an odd round operation.

A second pipeline register 140a temporarily stores output data of the second multiplexer 130a.

A secret key scheduler 150a generates secret keys for encrypting the 64-bit text data.

An FL1 block 160a operates output data of the first pipeline register 120a and the second pipeline register 140a and the secret key Ki from the secret key scheduler 150a with an FL function defined in the KASUMI encryption algorithm, and outputs 32-bit resultant data.

An FO block 170a has a three-stage pipeline structure including three pipeline registers 305, 305a, and 305b. The FO block 170a operates the output data of the FL1 block 160a and the second pipeline register 140a and the secret key Ki from the secret key scheduler 150a with an FI function defined in the KASUMI encryption algorithm and an exclusive-OR function, and outputs 32-bit resultant data.

An FL2 block 190a operates the even-round 32-bit output data of the FO block 170a and the secret key from the secret key scheduler 150a with the FL function defined in the KASUMI encryption algorithm, and outputs 32-bit data.

A first adder 180a of an adder section 180B exclusive-OR-gates the odd-rounded 32-bit output data of the FO block 170a and the output data of the second pipeline register 140a, and outputs the odd-rounded 32-bit data to the second multiplexer 130a.

A second adder 200a exclusive-OR-gates the output data of the FL2 block 190a and the output data of the first pipeline register 120a, and outputs the even-round 32-bit data to the first multiplexer 110a.

A third multiplexer 210a of an input/output control section 200B applies the output data of the FL1 block 160a to the FO block 170a in the odd round, and applies the output data of the second pipeline register 140a to the FO block 170a in the even round.

A fourth demultiplexer 220a applies the output data of the FO block 170a to the first adder 180a in the odd round, and applies the output data of the FO block 170a to the FL block 190a in the even round.

A first sync register 230a synchronizes an input time of the output data of the second pipeline register 140a inputted to the first adder 180a with an input time of the output data of the FO block 170a inputted to the first adder 180a via the fourth demultiplexer 220a.

A second sync register 240 synchronizes an input time of the output data of the FL2 block 190a inputted to the second adder 200a with an input time of the output data of the first pipeline register 120a.

Referring to FIG. 4, the FO block 170a has the three-stage pipeline structure composed of a fist pipeline section 310, a second pipeline section 320, and a third pipeline section 330, and thus a four-stage pipeline is constructed along with the first and second pipeline registers 120a and 140a.

The first pipeline section 310 stores upper 16-bit data of the 32-bit input data as upper 16-bit data of the first pipeline register by separating the upper 16-bit data into upper 9-bit data and lower 7-bit data and operating the 9-bit data and the 7-bit data with the FI function defined in the KASUMI encryption algorithm and the exclusive-OR function, and simultaneously stores the lower 16 bit data of the 32-bit input data as lower 16-bit data of the first pipeline register. Then, the first pipeline section 310 outputs 16-bit data by separating the upper 16-bit output data of the first pipeline register into upper 9-bit data and lower 7-bit data and operating the 9-bit data and the 7-bit data with the FI function defined in the KASUMI encryption algorithm, and then outputs the upper 16-bit data by exclusive-OR-gating the 16-bit output data and the lower 16-bit output data of the first pipeline register.

The second pipeline section 320 stores the upper 16-bit output data of the first pipeline register as upper 16-bit data of the second pipeline register, and simultaneously stores the lower 16-bit output data of the first pipeline register as lower 16-bit data of the second pipeline register by separating the lower 16-bit output data of the first pipeline register into upper 9-bit data and lower 7-bit data and operating the 9-bit data and the 7-bit data with the FI function defined in the KASUMI encryption algorithm and the exclusive-OR function. Then, the second pipeline section 320 outputs 16-bit data by separating the lower 16-bit output data of the second pipeline register into upper 9-bit data and lower 7-bit data and operating the 9-bit data and the 7-bit data with the FI function defined in the KASUMI encryption algorithm, and then outputs the lower 16-bit data by exclusive-OR-gating the 16-bit output data and the upper 16-bit output data of the second pipeline register.

The third pipeline section 330 stores the upper 16-bit data of the second pipeline register as upper 16-bit data of the third pipeline register by separating the upper 16-bit data of the second pipeline register into upper 9-bit data and lower 7-bit data and operating the 9-bit data and the 7-bit data with the FI function defined in

the KASUMI encryption algorithm and the exclusive-OR function, and simultaneously stores the lower 16 bit data of the second pipeline register as lower 16-bit data of the third pipeline register. Then, the third pipeline section 330 outputs 16-bit data by separating the upper 16-bit output data of the third pipeline register into upper 9-bit data and lower 7-bit data and operating the 9-bit data and the 7-bit data with the FI function defined in the KASUMI encryption algorithm, and then outputs the upper 16-bit data by exclusive-OR-gating the 16-bit output data and the lower 16-bit output data of the third pipeline register.

A first adder 301 of each pipeline section 310, 320, or 330 exclusive-OR-gates the upper or lower 16-bit data of the 32-bit input data and the secret key from the secret key scheduler 150a.

A first FI sub-block 302 of each pipeline section 310, 320, or 330 operates 16-bit output data of the first adder 301 with the FI function defined in the KASUMI encryption algorithm, and separates the 16-bit data into upper 9-bit data and lower 7-bit data.

A second adder 303 of each pipeline section 310, 320, or 330 exclusive-OR-gates the 9-bit data from the first FI sub-block 302 and the secret key from the secret key scheduler 105a.

A third adder 304 of each pipeline section 310, 320, or 330 exclusive-OR-gates the 7-bit data from the first FI sub-block 302 and the secret key from the secret key scheduler 105a.

Pipeline registers 305, 305a, and 305b of the pipeline sections 310, 320, and 330 store the 9-bit output data of the second adder 303 and the 7-bit output data of the third adder 304 as their upper 16-bit data, and temporarily store the lower or upper 16-bit data of the 32-bit input data.

A second FI sub-block 306 of each pipeline section 310, 320, or 330 operates the 9-bit data and the 7-bit data exclusive-OR-gated by the second adder 303 and the third adder 304 and then stored in the pipeline registers 305, 305a, and 305b with the FI function defined in the KASUMI encryption algorithm, and outputs 16-bit data.

A fourth adder 307 of each pipeline section 310, 320, or 330 exclusive-OR-gates the output data of the second FI sub-block 306 and the lower or upper 16-bit output data of the pipeline registers 305, 305a, and 305b, and outputs 16-bit data.

Referring to FIG. 5, an S9 box 410 of each FI sub-block 304 or 306 operates the upper 9-bit data of the 16-bit input data with a specified Boolean logical function in the KASUMI encryption algorithm.

A first adder 420 of each FI sub-block 304 or 306 exclusive-OR-gates the 9-bit output data of the S9 box 410 and 9-bit data obtained by performing an upper zero-bit extension function with respect to the lower 7 bits of the 16-bit input data, and outputs 9-bit data.

An S7 box 430 of the FI sub-block 304 or 306 operates the lower 7-bit data of the 16-bit input data with a specified Boolean logical function in the KASUMI encryption algorithm.

A second adder 440 of the FI sub-block 304 or 306 exclusive-OR-gates the 7-bit output data of the S7 box 430 and 7-bit data obtained by performing an upper bit truncation function with respect to the 9-bit output data of the first adder 420.

Referring to FIG. 6, the FO block 170a can be replaced by a one-stage pipeline structure having one pipeline section 540.

A first adder 510 of the FO block 170a OR-gates the upper 16-bit data of the 32-bit input data and the secret key from the secret key scheduler 150a.

A first FI block 520 of the FO block 170a operates 16-bit output data of the first adder 510 with the FI function defined in the KASUMI encryption algorithm.

A second adder 530 of the FO block 170a OR-gates 16-bit output data of the first FL block 520 and the lower 16-bit data of the 32-bit input data.

A pipeline section 540 of the FO block 170a is constructed in the same manner as the second pipeline section 320 illustrated in FIG. 5.

The pipeline section 540 stores the upper 16-bit output data of the second adder 530 as upper 16-bit data of the pipeline register 305a, and simultaneously stores the lower 16-bit data of the 32-bit input data as lower 16-bit data of the pipeline register 305 by separating the lower 16-bit data of the 32-bit input data into upper 9-bit data and lower 7-bit data and operating the 9-bit data and the 7-bit data with the FI function defined in the KASUMI encryption algorithm and the exclusive-OR function. Then, the pipeline section 540 outputs 16-bit data by separating the lower 16-bit output data of the pipeline register 305a into upper 9-bit data and lower 7-bit data and operating the 9-bit data and the 7-bit data with the FI function defined in the KASUMI encryption algorithm, and then outputs the 16-bit output data as the lower 16-bit data by exclusive-OR-gating the 16-bit output data and the upper 16-bit output data of the pipeline register 305a.

A third adder 550 of the FO block 170a OR-gates the upper 16-bit output data of the pipeline register 305a and the secret key from the secret key scheduler 150a.

A second FI block 560 of the FO block 170a operates 16-bit output data of the third adder 550 with the FI function defined in the KASUMI encryption algorithm.

A fourth adder 570 of the FO block 170a OR-gates 16-bit output data of the second FL block 560 and the lower 16-bit output data of the pipeline section 540.

Referring to FIG. 7, a C-constant register 155 of the secret key scheduler 150a stores 8 C-constant values of 16 bits defined for key scheduling in the KASUMI encryption algorithm, and whenever four clocks are generated, one C-constant value rotates to the left side.

A secret key register 156 of the secret key scheduler 150a stores 32 (=4×8) secret key values of 16 bits KA1~KD8 defined by the user, and whenever one clock is generated, one secret key value rotates.

The time for the rotation of four secret key values is synchronized with the time for the rotation of one C-constant value to the left side.

A plurality of rotators 157, 157a, 157b, 157c, and 157d of the secret key scheduler 150a generate specified secret keys by rotating the specified secret key values of the secret key register 152a to the left side as many as the determined number of bits, respectively.

The five rotators 157, 157a, 157b, 157c, and 157d as shown in FIG. 7 generate the secret keys KLi1, KOi1, KOi2, KOi3, and KL1_even by rotating the initial secret key values KA1, KA2, KD5, KC6, and KC8 stored in the secret key register 156 to the left side by 1 bit, 5 bits, 8 bits, 13 bits, and 1 bit, respectively.

A plurality of adders 158, 158a, 158b, 158c, and 158d of the secret key scheduler 150s generate the secret keys by exclusive-OR-gating the specified secret key values of the secret key register 156 and the corresponding C-constant values, respectively.

The five adders 158, 158a, 158b, 158c, and 158d as shown in FIG. 7 generate the secret keys KL2_even, KLi2, KIi1, Kii1, and KIi3 by exclusive-OR-gating the initial secret key values KB2, KA3, KD3, KA5, and KC7 stored in the secret key register 156 and the corresponding C-constant values C3, C3, C4, C5, and C8, respectively.

A plurality of sync registers 159, 159a, and 159b of the secret key scheduler 150a synchronize the input time of the C-constant values inputted to the adders 158, 158a, 158b, 158c, and 158d with the input time of the secret key values.

The three sync registers 159, 159a, and 159b illustrated in FIG. 7 synchronize the input time of the C-constant values C3, C4, and C8 respectively inputted to the first adder 158, the second adder 158b, and the fifth adder 158d with the input time of the secret key values KB2, KD3, and KC7 corresponding to the C-constant values C3, C4, and C8.

Referring to FIG. 8, the secret key scheduler 150a can be replaced by a secret key scheduler composed of four secret key schedulers 150 illustrated in FIG. 2 and five multiplexers 150a1, 150a2, 150a3, 150a4, and 150a5.

32 secret key values KL1-0~KI3-3 outputted from the four secret key schedulers 150 are applied to the five multiplexers 150a1, 150a2, 150a3, 150a4, and 150a5 the outputs of which are controlled by a 2-bit select signal Key_sel, and then the secret key values required for the encryption apparatus illustrated in FIG. 3 are finally generated.

The encryption apparatus applying the KASUMI encryption algorithm as constructed above according to another embodiment of the present invention operates as follows.

In order to heighten the data throughput, the encryption apparatus illustrated in FIG. 3 comprises a round circuit that applies a four-stage pipeline structure using the first or second pipeline register 110a or 130a and the FO block 170a having the three-stage pipeline structure as shown in FIGs. 3, 4, and 5, and the secret key scheduler 150a. A four-round operation is performed for one clock cycle, and the encryption apparatus encrypts four 64-bit text input data by repeatedly performing the round operation eight times in all.

Initially, the upper 32-bit data of the 64-bit text input data is inputted to the first multiplexer 110a through an initial input port 111a, and simultaneously the lower 32-bit data of the 64-bit text input data is inputted to the second multiplexer 130a through an initial input port 131a.

At this time, the upper 32-bit data inputted to the first multiplexer 110a is stored in the first pipeline register 120a via the first multiplexer 110a as indicated as a solid line in FIG. 3. Also, the upper 32-bit data sequentially passes through the FL1 block 160a, third multiplexer 210a, F0 block 170a, and fourth demultiplexer 220a, and then exclusive-OR-gated with the lower 32-bit data stored in the second

pipeline register 140a by the first adder 180a and synchronized with the input time by the first sync register 230a. The exclusive-OR-gated data is then inputted to an odd-round performing result data input port 132a of the second multiplexer 130a.

The 32-bit data exclusive-OR-gated by the first adder 180a and inputted to the second multiplexer 130a is newly stored in the second pipeline register 140a via the second multiplexer 130a.

The upper 32-bit data newly stored in the second pipeline register 140a, as shown as a dotted line in FIG. 3, sequentially passes through the third multiplexer 210a, FO block 170a, fourth demultiplexer 220a, and FL2 block 190a, and then exclusive-OR-gated with the upper 32-bit data stored in the first pipeline register 120a by the second adder 200a and synchronized with the input time by the second sync register 240. The exclusive-OR-gated data is then inputted to an even-rounding resultant data input port 112a of the first multiplexer 110a.

The 32-bit data exclusive-OR-gated by the second adder 200a and inputted to the first multiplexer 110a is newly stored in the first pipeline register 120a via the first multiplexer 110a.

The operating procedure until the 32-bit data is newly stored in the first pipeline register 120a as described above is the one-round operation procedure that is performed for one clock cycle with respect to one 64-bit text data. By performing the round operation eight times with respect to four 64-bit text data, four 64-bit text input data can be encrypted.

If the FO block 170a in the encryption apparatus illustrated in FIG. 3 is replaced by the FO block having the one-stage pipeline structure illustrated in FIG. 6, the encryption apparatus is composed of the round circuit applying the two-stage pipeline and the secret key scheduler 150a. This encryption apparatus perform the two-round operation for one clock cycle, and encrypts two 64-bit text data by repeatedly performing the round operation eight times in all.

Meanwhile, by combining the encryption apparatus having the round circuit composed of the FL block and the FO block as shown in FIG. 1 (i.e., the first embodiment) with the encryption apparatus having the round circuit composed of the FL block and the FO block of the three-stage or one-stage pipeline structure as shown in FIG. 3 (i.e., the second embodiment), diverse encryption apparatuses that apply the KASUMI encryption algorithm can be newly implemented.

An encryption apparatus illustrated in FIG. 9 has a two-round circuit composed of FL blocks 610 and 650 and FO blocks 620 and 640, and encrypts 64-bit text input data by performing a two-round operation for one clock cycle.

The encryption apparatus comprises registers 600 and 670 for storing the 64-bit data, an FL1 block 610 for performing an odd round, an FO1 block 620 for performing an odd round, an FO2 block 640 for performing an even round, an FL2 block 650 for performing an even round, and adders 630 and 660 for performing an exclusive-OR function.

By adding a round circuit composed of an FL block and an FO block to the two-round circuit, an encryption apparatus that performs a three to eight round operation for one clock cycle can be implemented.

An encryption apparatus illustrated in FIG. 10 includes a two-round circuit having a two-stage pipeline structure by adding pipeline registers 631 and 661 to the encryption apparatus of FIG. 9 in order to heighten the data throughput. This encryption apparatus encrypts two different 64-bit text data by performing the two-round operation for one clock cycle.

By extending the two-round circuit having the two-stage pipeline structure to the 8-round circuit having the 8-stage pipeline structure, an encryption apparatus that performs 8 different 64-bit text input data in parallel can be implemented.

An encryption apparatus illustrated in FIG. 11 has a two-round circuit having a four-stage pipeline structure by replacing the FO block of the encryption apparatus illustrated in FIG. 10 by the FO block having the one-stage pipeline structure illustrated in FIG. 6. The hardwired structure of this encryption apparatus is somewhat complicated, but the operational clock frequency and the data throughput are heightened.

This encryption apparatus comprises registers 600a and 670a for storing the 64-bit data and acting as pipeline registers, an odd-round FL1 block 610a, an odd-round FO1 block 620a including the pipeline register 305a, an even-round L2 block 650a, an even-round FO2 block 640a including the pipeline register 305a, adders 630a and 660a for performing an exclusive-OR function, sync registers 631a, 631c, and 661a for synchronizing the input time of data to the adders 630a and 660a, and a pipeline register 631b.

An encryption apparatus illustrated in FIG. 12 has a two-round circuit having an eight-stage pipeline structure by replacing the FO block having the one-stage pipeline structure illustrated in FIG. 11 by the FO block having the three-stage

pipeline structure illustrated in FIGs. 3 to 5. This encryption apparatus has the operational clock frequency and the data throughput higher than those of the encryption apparatus illustrated in FIG. 11.

The whole construction of this encryption apparatus is equal to that of the encryption apparatus illustrated in FIG. 11, and only FO1 block 620b, FO2 block 640b, and sync registers 631d, 631e, and 661f have different constructions from those of the encryption apparatus of FIG. 11.

Also, by combining in parallel two or more encryption apparatuses diversely implemented as described above according to the present invention, a multiple encryption apparatus that can encrypt different text data can be implemented.

Industrial Applicability

As apparent from the above description, according to the encryption apparatus applying a KASUMI encryption algorithm according to the present invention, a round circuit is constructed through combination of an FL block with an FO block which separate a secret key defined in the KASUMI encryption algorithm and provided from a secret key scheduler and 64-bit text data into 32-bit data and perform a specified encryption operation function, and the FO block is constructed by a multistage pipeline using a plurality of pipeline registers. Thus, the encryption apparatus has a low power consumption, and is small-sized in comparison to the conventional encryption apparatus using the MISTY encryption algorithm or the DES encryption algorithm. Also, the encryption apparatus according to the present invention can be applied to portable terminals or high-performance servers that require the low power consumption and the small size.

The forgoing embodiments are merely exemplary and are not to be construed as limiting the present invention. The present teachings can be readily applied to other types of apparatuses. The description of the present invention is intended to be illustrative, and not to limit the scope of the claims. Many alternatives, modifications, and variations will be apparent to those skilled in the art.

Claims

1. An encryption apparatus applying a KASUMI encryption algorithm comprising:

a register section for selecting and storing either of text data and input data obtained after performing a round operation;

a secret key scheduler for generating secret keys for encrypting the text data;

an FL block for operating output data of the register section and the secret key with an FL function defined in the KASUMI encryption algorithm;

an FO block for operating the output data of the register section and the secret key with an FI function defined in the KASUMI encryption algorithm and an exclusive-OR function;

an adder section for exclusive-OR-gating output data of the FL block and the FO block and the output data of the register section and applying exclusive-OR-gated data to the register section; and

an input/output control section for selecting the input data of the FL block and the FO block and selecting paths of the output data of the FL block and the FO block.

2. The encryption apparatus of claim 1, wherein the register section comprises:

a first multiplexer for selecting and outputting either of upper 32-bit input data of the 64-bit text data and 32-bit input data obtained after performing an even round operation;

a first register for temporarily storing output data of the first multiplexer;

a second multiplexer for selecting and outputting either of lower 32-bit input data of the 64-bit text data and 32-bit input data obtained after performing an odd round operation; and

a second register for temporarily storing output data of the second multiplexer.

3. The encryption apparatus of claim 1, wherein the secret key scheduler comprises:

a C-constant register for storing 8 C-constant values of 16 bits defined for key scheduling in the KASUMI encryption algorithm, wherein whenever one clock is generated, one C-constant value rotates to the left side;

a secret key register for storing 8 secret key values of 16 bits defined by a user, wherein whenever one clock is generated, one secret key value rotates;

a plurality of rotators for generating specified secret keys by rotating the specified secret key values of the secret key register to the left side as many as the determined number of bits, respectively; and

a plurality of adders for generating the secret key by exclusive-OR-gating the specified secret key values of the secret key register and the corresponding C-constant values, respectively.

4. The encryption apparatus of claim 1, wherein the adder section comprises:

a first adder for exclusive-OR-gating the even-round 32-bit output data of the FL block and the output data of the first register, and outputting the even-round 32-bit data to the first multiplexer; and

a second adder for exclusive-OR-gating the odd-round 32-bit output data of the FO block and the output data of the second register, and outputting the odd-round 32-bit data to the second multiplexer.

5. The encryption apparatus of claim 1, wherein the input/output control section comprises:

a third multiplexer for applying the output data of the first register to the FL block in the odd round, and applying the output data of the FO block to the FL block in the even round;

a fourth multiplexer for applying the output data of the FL block to the FO block in the odd round, and applying the output data of the second register to the FO block in the even round;

a fifth multiplexer for applying the output data of the FL block to the fourth multiplexer in the odd round, and applying the output data of the FL block to the first adder in the even round; and

a sixth multiplexer for applying the output data of the FO block to a second adder in the odd round, and applying the output data of the FO block to the third multiplexer in the even round.

6. An encryption apparatus applying a KASUMI encryption algorithm comprising:

a pipeline register section for selecting and storing either of text data and input data obtained after performing a round operation;

a secret key scheduler for generating secret keys for encrypting the text data;

an FL1 block for operating output data of the pipeline register section and the secret key with an FL function defined in the KASUMI encryption algorithm;

an FO block having a three-stage pipeline structure, and operating output data of the FL1 block and the pipeline register section and the secret key with an FI function defined in the KASUMI encryption algorithm and an exclusive-OR function;

an FL2 block for operating output data of the FO block and the secret key with the FL function defined in the KASUMI encryption algorithm;

an adder section for exclusive-OR-gating the output data of the FO block and the FL2 block and the output data of the pipeline register section so that the output data of the FO block and the FL2 block is synchronized with the output data of the pipeline register section, and applying exclusive-OR-gated data to the pipeline register section; and

an input/output control section for selecting the input data of the FO block and selecting a path of the output data of the FO block.

7. The encryption apparatus of claim 6, wherein the pipeline register section comprises:

a first multiplexer for selecting and outputting either of upper 32-bit input data of the 64-bit text data and 32-bit input data obtained after performing an even round operation.

a first pipeline register for temporarily storing output data of the first multiplexer;

a second multiplexer for selecting and outputting either of lower 32-bit input data of the 64-bit text data and 32-bit input data obtained after performing an odd round operation; and

a second pipeline register for temporarily storing output data of the second multiplexer.

8. The encryption apparatus of claim 6, wherein the FO block includes three pipeline sections each of which comprises:

a first adder for exclusive-OR-gating upper or lower 16-bit data of 32-bit input data and the secret key from the secret key scheduler;

a first FI sub-block for operating 16-bit output data of the first adder with the FI function defined in the KASUMI encryption algorithm, and separating the 16-bit data into upper 9-bit data and lower 7-bit data;

a second adder for exclusive-OR-gating the 9-bit data from the first FI sub-block and the secret key from the secret key scheduler;

a third adder for exclusive-OR-gating the 7-bit data from the first FI sub-block and the secret key from the secret key scheduler;

a pipeline register for storing the 9-bit output data of the second adder and the 7-bit output data of the third adder as its upper 16-bit data, and temporarily storing the lower or upper 16-bit data of the 32-bit input data;

a second FI sub-block for operating the 9-bit data and the 7-bit data exclusive-OR-gated by the second and third adders and then stored in the pipeline register with the FI function defined in the KASUMI encryption algorithm, and outputting 16-bit data; and

a fourth adder for exclusive-OR-gating the output data of the second FI sub-block and the lower or upper 16-bit output data of the pipeline register, and outputting 16-bit data.

9. The encryption apparatus of claim 8, wherein the FI sub-block comprises:

an S9 box for operating the upper 9-bit data of the 16-bit input data with a specified Boolean logical function in the KASUMI encryption algorithm;

a first adder for exclusive-OR-gating 9-bit output data of the S9 box and 9-bit data obtained by performing an upper zero-bit extension function with respect to the lower 7 bits of the 16-bit input data, and outputting 9-bit data;

an S7 box for operating the lower 7-bit data of the 16-bit input data with a specified Boolean logical function in the KASUMI encryption algorithm; and

a second adder for exclusive-OR-gating 7-bit output data of the S7 box and 7-bit data obtained by performing an upper-bit truncation function with respect to the 9-bit output data of the first adder.

10. The encryption apparatus of claim 6, wherein the adder section comprises:

a first adder for exclusive-OR-gating odd-round 32-bit output data of the FO block and output data of a first register, and outputting odd-round 32-bit data to a second multiplexer; and

a second adder for exclusive-OR-gating output data of the FL2 block and output data of a first pipeline register, and outputting even-round 32-bit data to a first multiplexer.

11. The encryption apparatus of claim 6, wherein the input/output control section comprises:

a third multiplexer for applying output data of the FL1 block to the FO block in the odd round, and applying output data of a second pipeline register to the FO block in the even round; and

a fourth multiplexer for applying the output data of the FO block to a first adder in the odd round, and applying output data of the FO block to the FL2 block in the even round.

12. The encryption apparatus of claim 6, wherein an input time of the output data of the pipeline register section is synchronized with an input time of the output data of the FO block inputted to the adder section via the input/output control section by a sync register.

13. The encryption apparatus of claim 12, wherein the sync register comprises:

a first register for synchronizing an input time of output data of a second pipeline register inputted to a first adder with an input time of the output data of the FO block inputted to the first adder via a fourth demultiplexer; and

a second sync register for synchronizing an input time of the output data of the FL2 block inputted to a second adder with an input time of output data of a first pipeline register.

14. The encryption apparatus of claim 6, wherein the FO block comprises:

a first adder for OR-gating upper 16-bit data of 32-bit input data and the secret key from the secret key scheduler;

a first FI block for operating 16-bit output data of the first adder with the FI function defined in the KASUMI encryption algorithm;

a second adder for OR-gating 16-bit output data of the FL1 block and lower 16-bit data of the 32-bit input data;

a pipeline section for storing 16-bit output data of the second adder as upper 16-bit data of the pipeline register, operating lower 16-bit output data of the 32-bit input data with the FI function defined in the KASUMI algorithm and an exclusive-OR function when storing and outputting the lower 16-bit output data, and exclusive-OR-gating the lower 16-bit output data of the pipeline register and the upper 16-bit output data to output lower 16-bit data;

a third adder for OR-gating the upper 16-bit output data of the pipeline register and the secret key from the secret key scheduler;

a second FI block for operating 16-bit output data of the third adder with the FI function defined in the KASUMI encryption algorithm; and

a fourth adder for OR-gating the 16-bit output data of the second FL block and the lower 16-bit output data of the pipeline section.

15. The encryption apparatus of claim 6, wherein the secret key scheduler comprises:

a C-constant register for storing 8 C-constant values of 16 bits defined for key scheduling in the KASUMI encryption algorithm, wherein whenever four clocks are generated, one C-constant value rotates to the left side;

a secret key register for storing 16-bit secret key values defined by a user, wherein whenever one clock is generated, one secret key value rotates;

a plurality of rotators for generating specified secret keys by rotating the specified secret key values of the secret key register to the left side as many as the determined number of bits, respectively;

a plurality of adders for generating the secret keys by exclusive-OR-gating the specified secret key values of the secret key register and the corresponding C-constant values, respectively; and

a plurality of sync registers for synchronizing an input time of the C-constant values inputted to the adders with an input time of the secret keys.

FIG.1

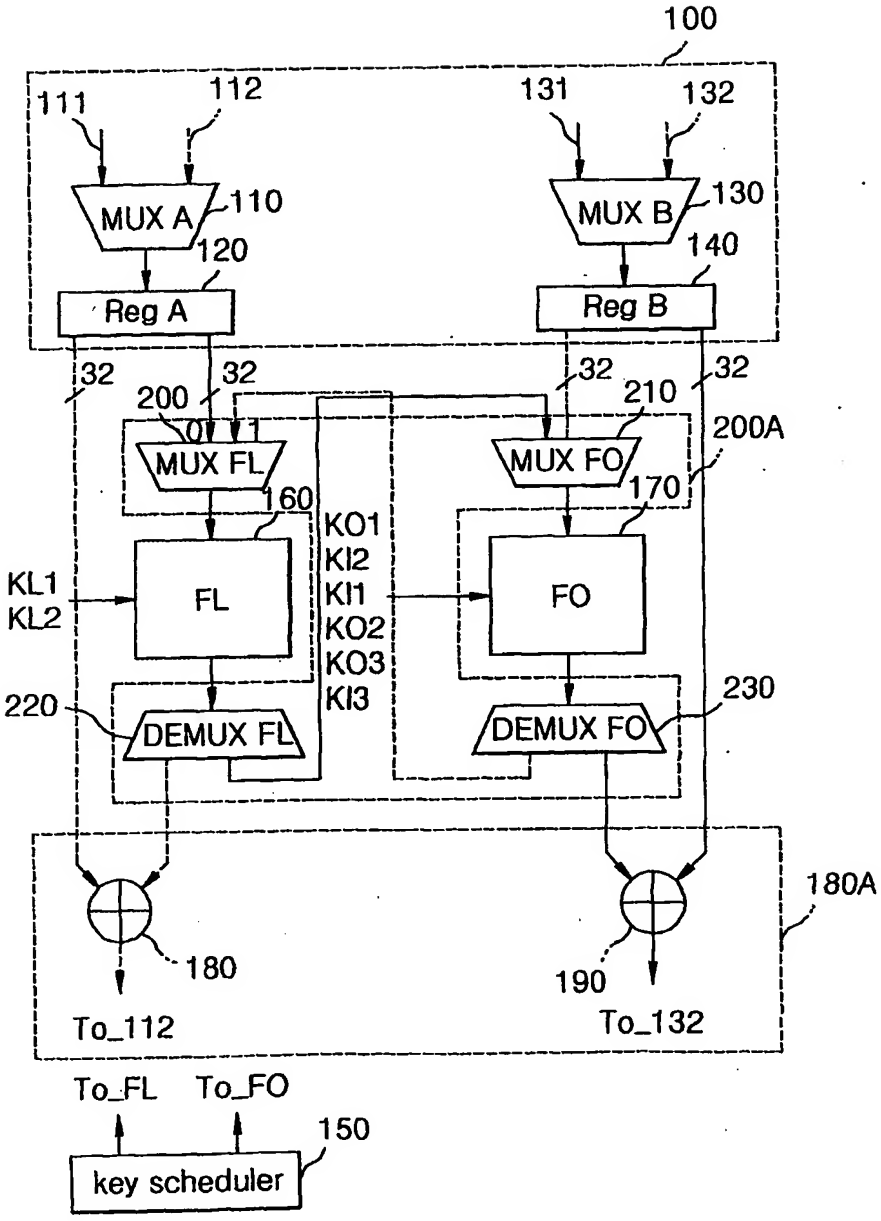

100
111
112
131
132
MUX A
110
MUX B
130
120
140
Reg A
Reg B
32
32
32
32
200
210
200A
0
1
MUX FL
MUX FO
160
170
KO1
KI2
KI1
KO2
KO3
KI3
KL1
KL2
FL
FO
220
DEMUX FL
DEMUX FO
230
180A
180
190
To_112
To_132
To_FL
To_FO
150
key scheduler

FIG.2

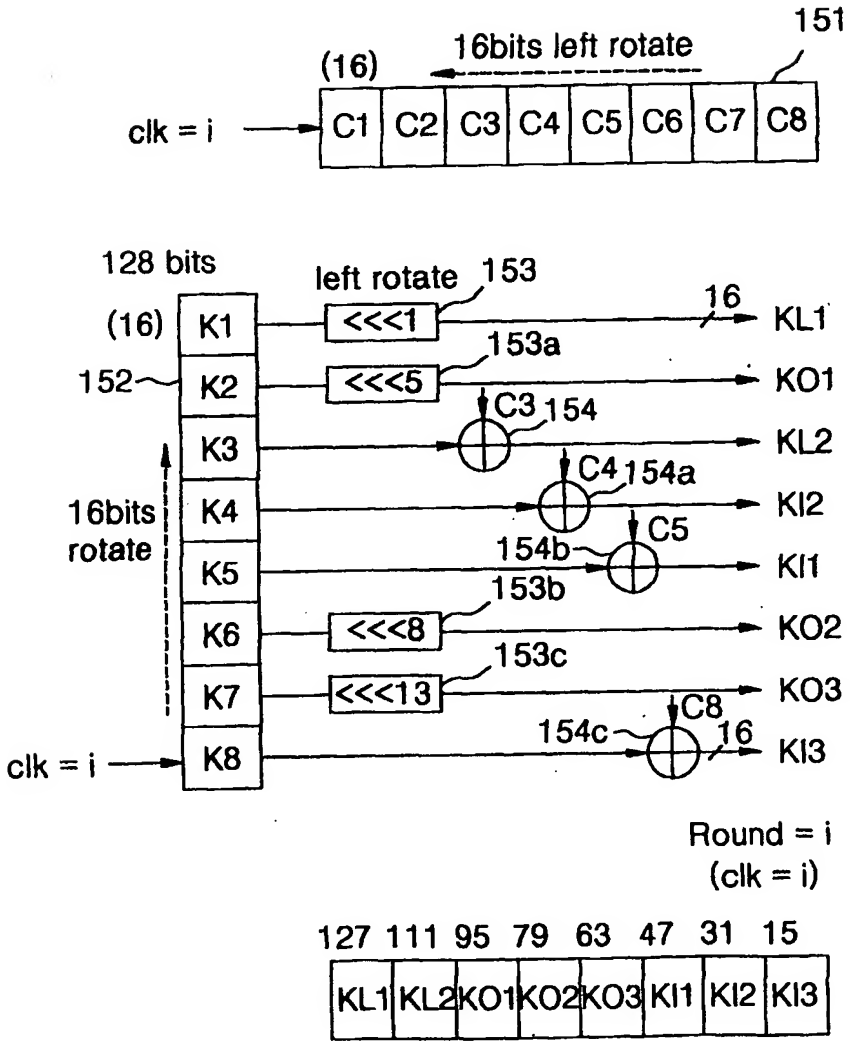

151
16bits left rotate
(16)
clk = i
C1
C2
C3
C4
C5
C6
C7
C8
128 bits
left rotate
153
(16)
K1
<<<1
16
KL1
152
K2
153a
<<<5
KO1
C3
154
K3
KL2
C4
154a
16bits
rotate
K4
KI2
C5
154b
K5
KI1
153b
K6
<<<8
KO2
153c
K7
<<<13
KO3
C8
154c
16
clk = i
K8
KI3
Round = i
(clk = i)
127 111 95 79 63 47 31 15
KL1
KL2
KO1
KO2
KO3
KI1
KI2
KI3

FIG.3

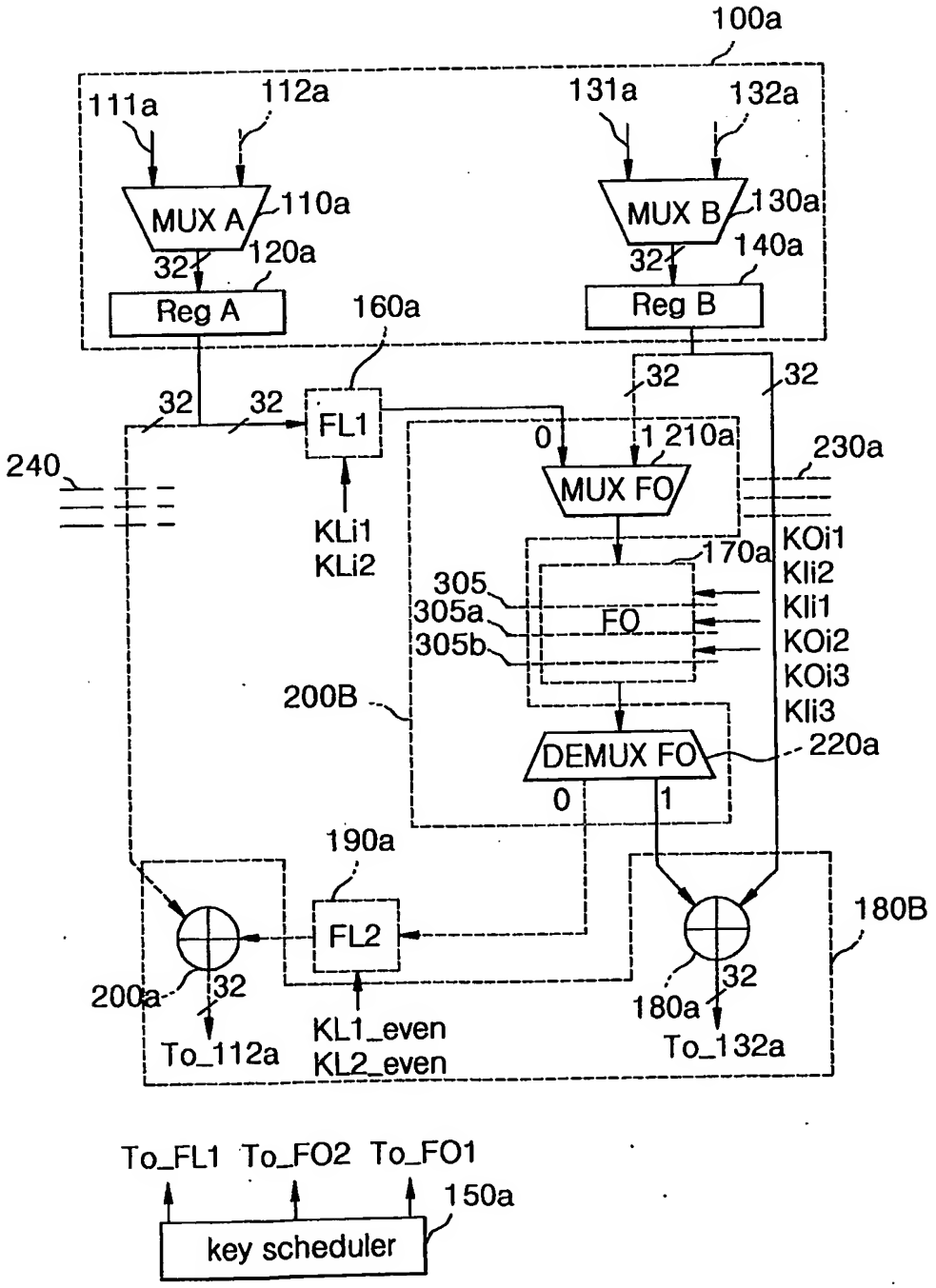

100a
111a
112a
131a
132a
MUX A
110a
MUX B
130a
32
120a
32
140a
Reg A
160a
Reg B
32
32
32
32
FL1
0
1
210a
230a
240
MUX FO
KLi1
KLi2
170a
KOi1
Kli2
305
305a
305b
FO
Kli1
KOi2
KOi3
Kli3
200B
DEMUX FO
220a
0
1
190a
180B
FL2
200a
32
32
180a
To_112a
KL1_even
KL2_even
To_132a
To_FL1
To_FO2
To_FO1
150a
key scheduler

FIG.4

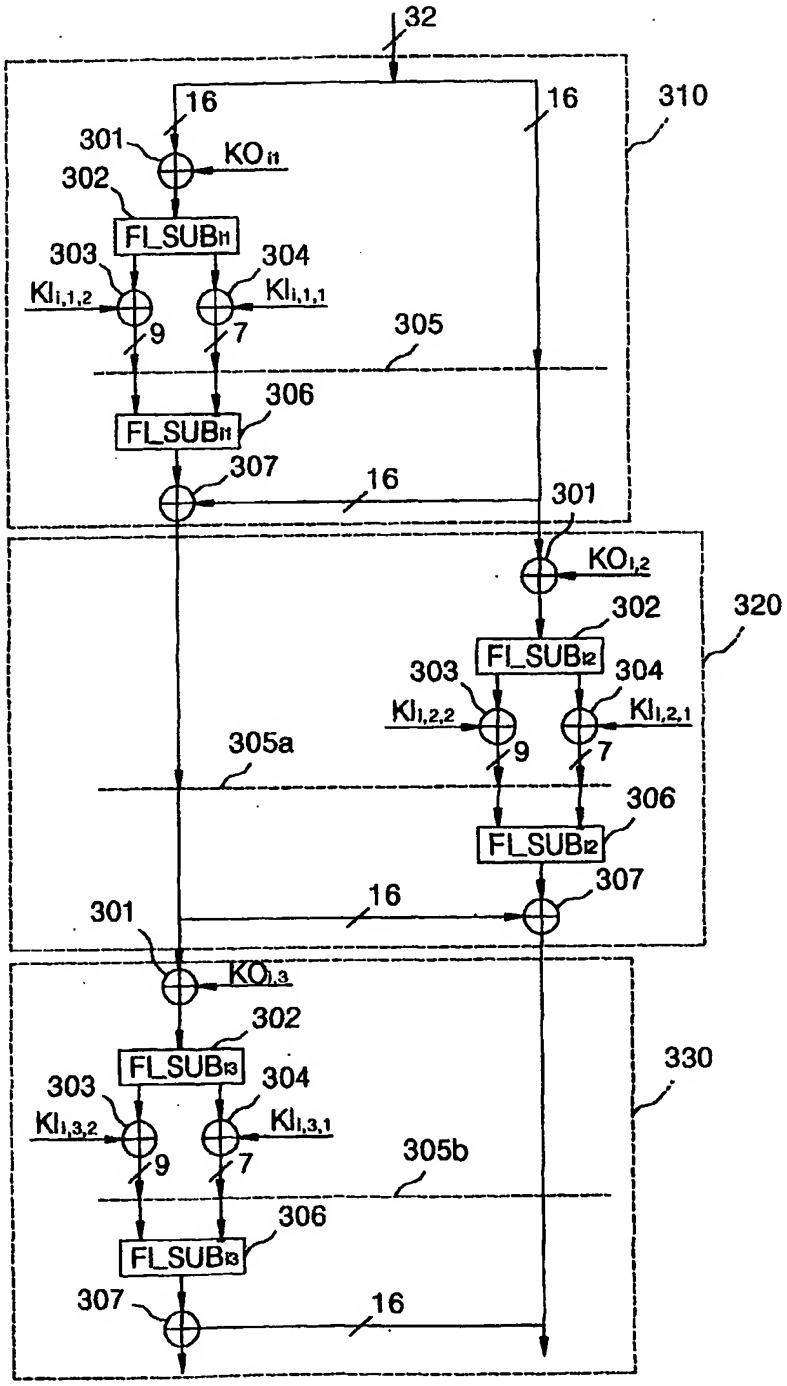

32
16
16
310
301
KO11
302
FL_SUB11
303
304
KI1,1,2
KI1,1,1
9
7
305
306
FL_SUB11
307
16
301
KO1,2
320
302
FL_SUB12
303
304
KI1,2,2
KI1,2,1
9
7
305a
306
FL_SUB12
307
16
301
KO1,3
302
FL_SUB13
330
303
304
KI1,3,2
KI1,3,1
9
7
305b
306
FL_SUB13
307
16

FIG.5

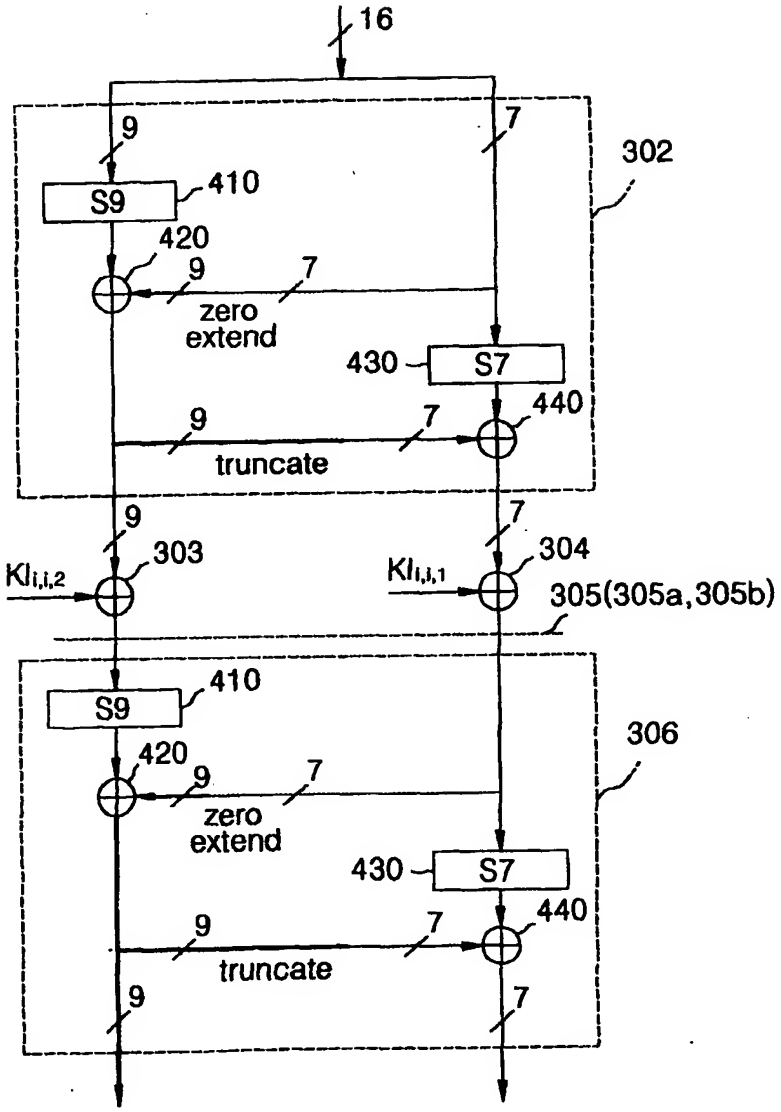

16
9
7
302
S9
410
420
9
7
zero
extend
430
S7
440
9
7
truncate
9
7
303
304
$KI_{i,j,2}$
$KI_{i,j,1}$
305(305a,305b)
S9
410
306
420
9
7
zero
extend
430
S7
440
9
7
truncate
9
7

FIG.6

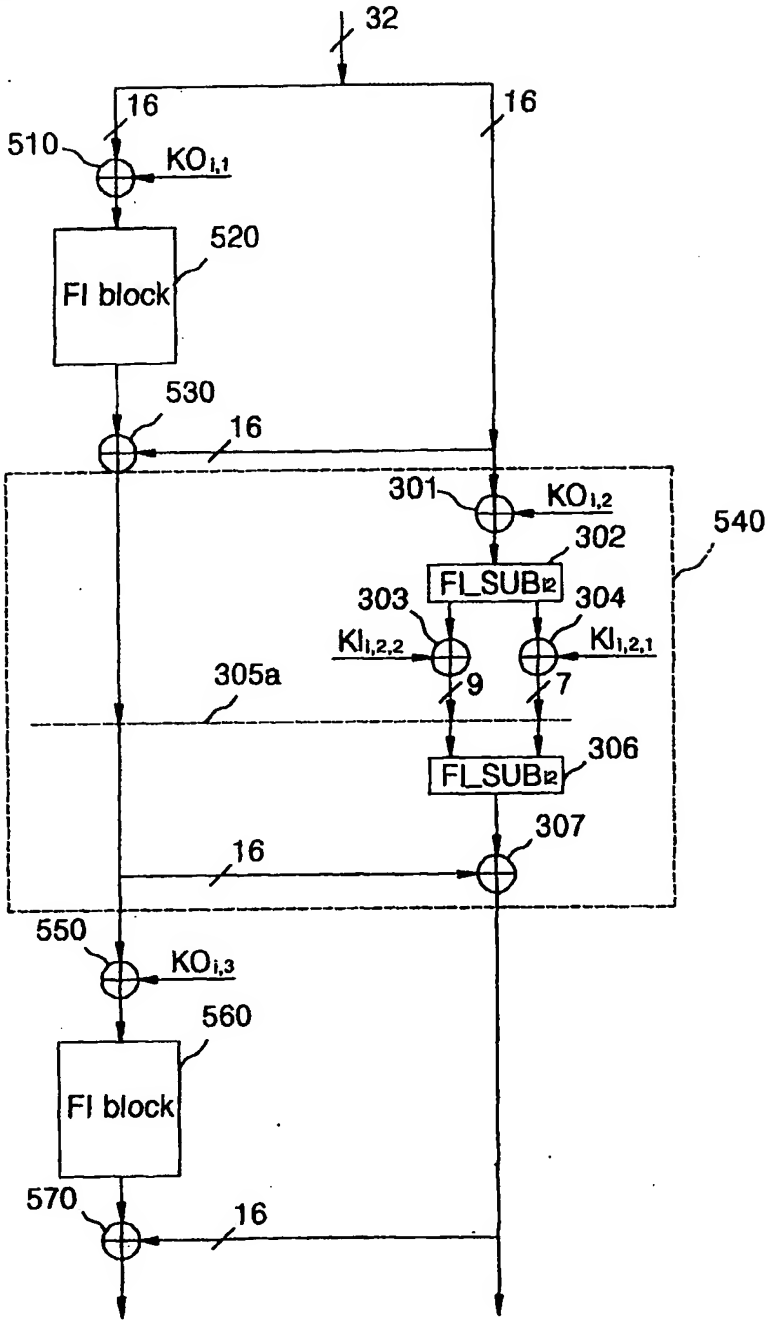

32
16
16
510
$KO_{i,1}$
520
FI block
530
16
301
$KO_{i,2}$
540
302
FL_SUB_{12}
303
304
$KI_{i,2,2}$
$KI_{i,2,1}$
9
7
305a
306
FL_SUB_{12}
307
16
550
$KO_{i,3}$
560
FI block
570
16

FIG.7

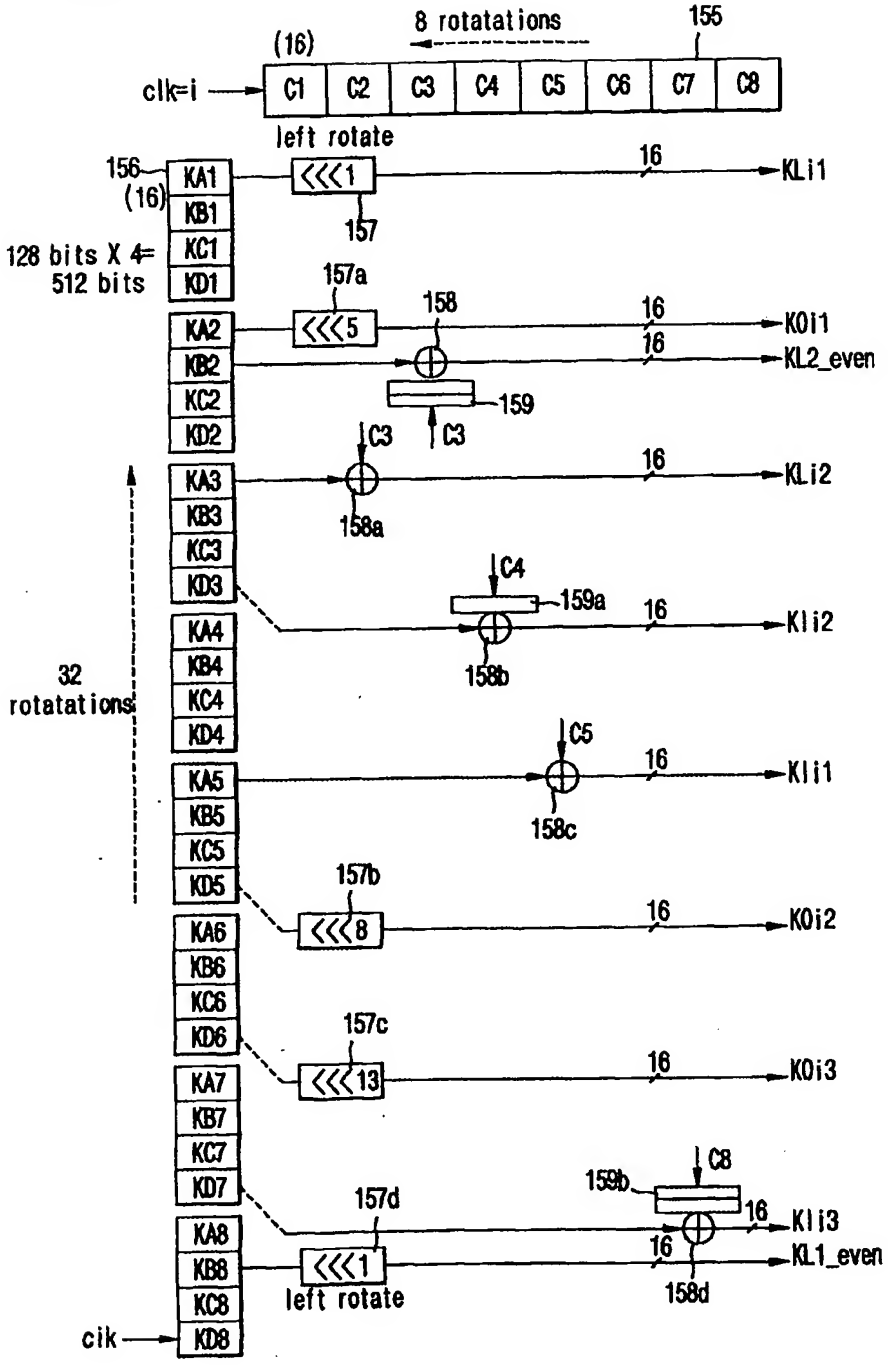

8 rotatations
155
(16)
clk=i
C1
C2
C3
C4
C5
C6
C7
C8
left rotate
156
(16)
KA1
KB1
KC1
KD1
128 bits X 4=
512 bits
<<<1
16
KLi1
157
157a
<<<5
158
16
KOi1
16
KL2_even
KA2
KB2
KC2
KD2
159
C3
C3
KA3
KB3
KC3
KD3
16
KLi2
158a
C4
159a
16
Kli2
158b
32
rotatations
KA4
KB4
KC4
KD4
C5
16
Kli1
158c
KA5
KB5
KC5
KD5
157b
<<<8
16
KOi2
KA6
KB6
KC6
KD6
157c
<<<13
16
KOi3
KA7
KB7
KC7
KD7
C8
159b
157d
16
Kli3
16
KL1_even
KA8
KB8
KC8
KD8
<<<1
left rotate
158d
clk

FIG.8

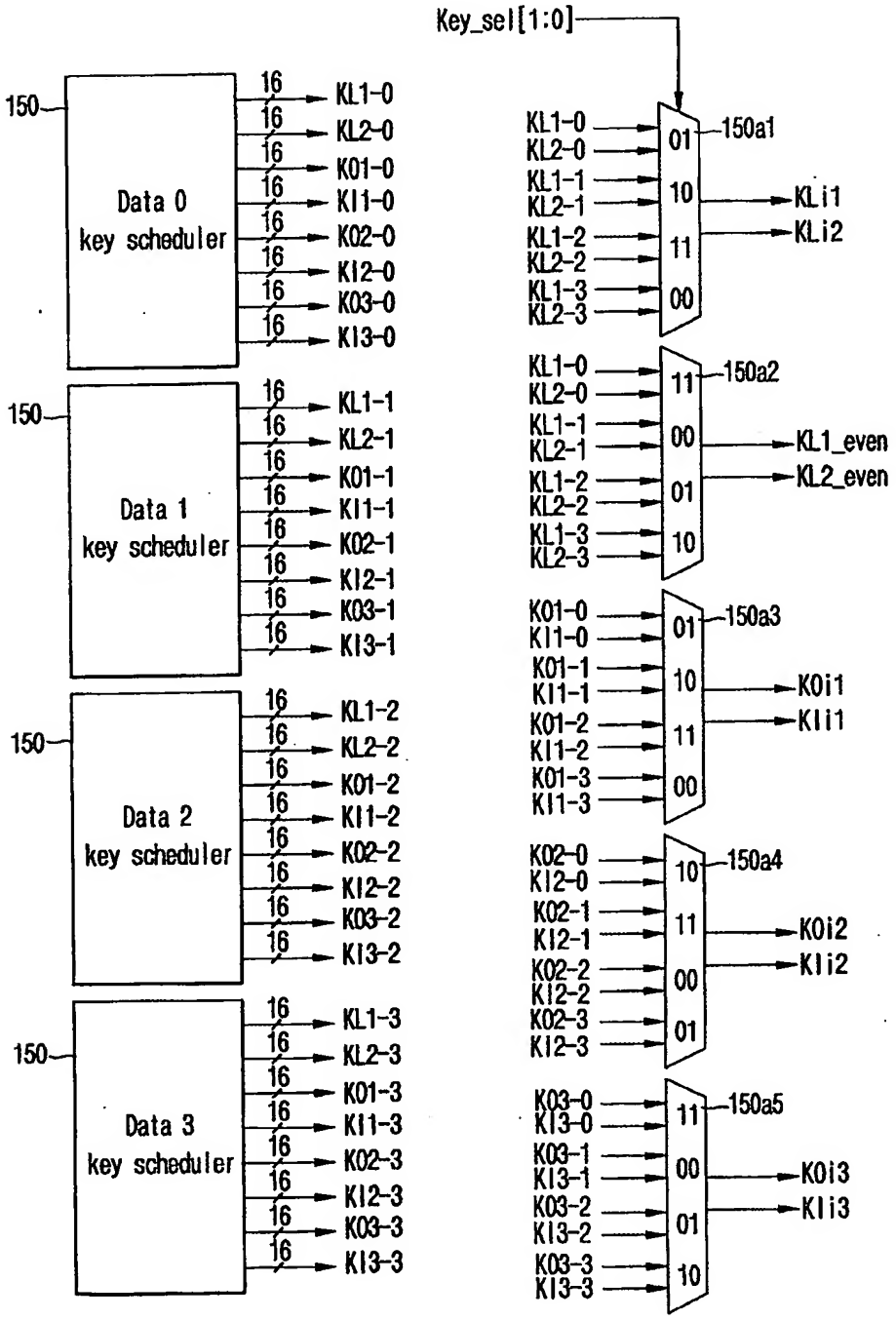

Key_sel[1:0]
150
Data 0 key scheduler
KL1-0
KL2-0
KO1-0
KI1-0
KO2-0
KI2-0
KO3-0
KI3-0
150
Data 1 key scheduler
KL1-1
KL2-1
KO1-1
KI1-1
KO2-1
KI2-1
KO3-1
KI3-1
150
Data 2 key scheduler
KL1-2
KL2-2
KO1-2
KI1-2
KO2-2
KI2-2
KO3-2
KI3-2
150
Data 3 key scheduler
KL1-3
KL2-3
KO1-3
KI1-3
KO2-3
KI2-3
KO3-3
KI3-3
16
150a1
01
10
11
00
KLi1
KLi2
150a2
11
00
01
10
KL1_even
KL2_even
150a3
01
10
11
00
KOi1
KIi1
150a4
10
11
00
01
KOi2
KIi2
150a5
11
00
01
10
KOi3
KIi3

FIG.9

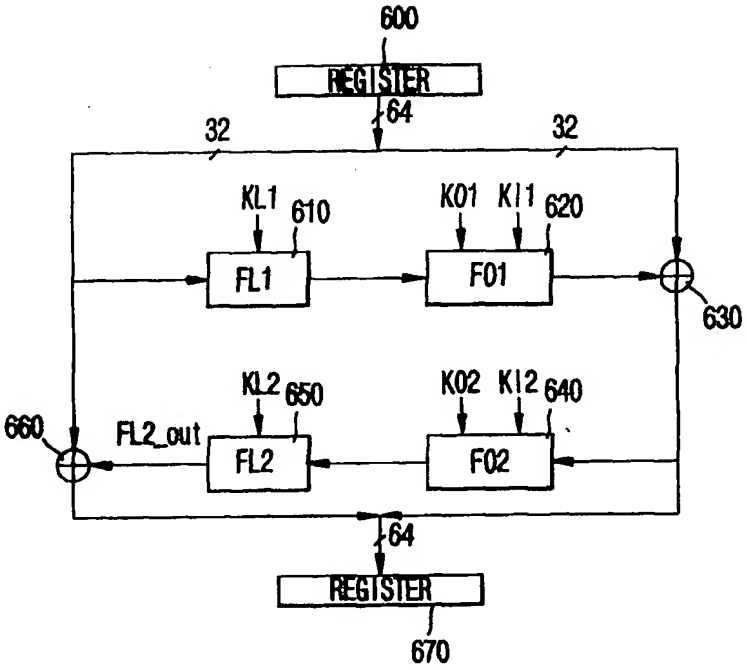

600
REGISTER
64
32
32
KL1
610
K01
KI1
620
FL1
F01
630
KL2
650
K02
KI2
640
660
FL2_out
FL2
F02
64
REGISTER
670

FIG.10

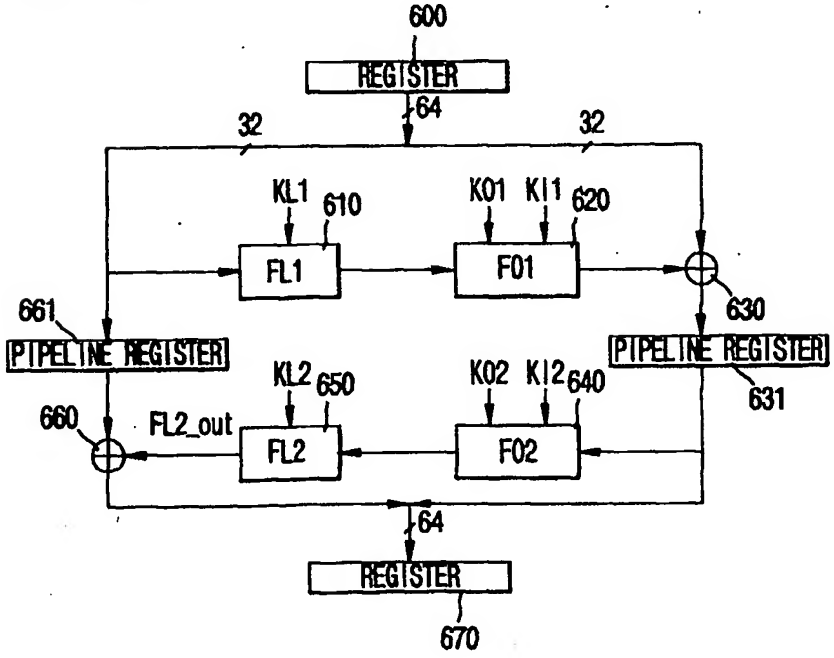

600
REGISTER
64
32
32
KL1
610
K01
KI1
620
FL1
F01
630
661
PIPELINE REGISTER
PIPELINE REGISTER
631
KL2
650
K02
KI2
640
660
FL2_out
FL2
F02
64
REGISTER
670

FIG.11

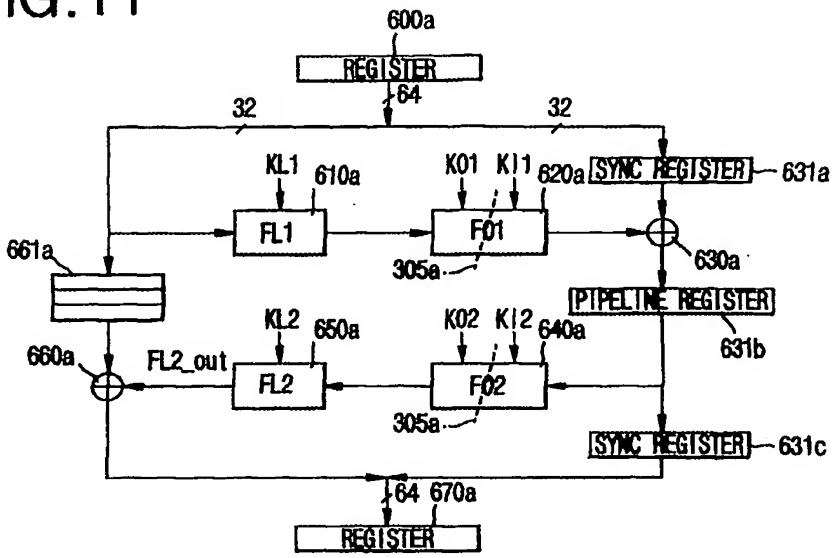
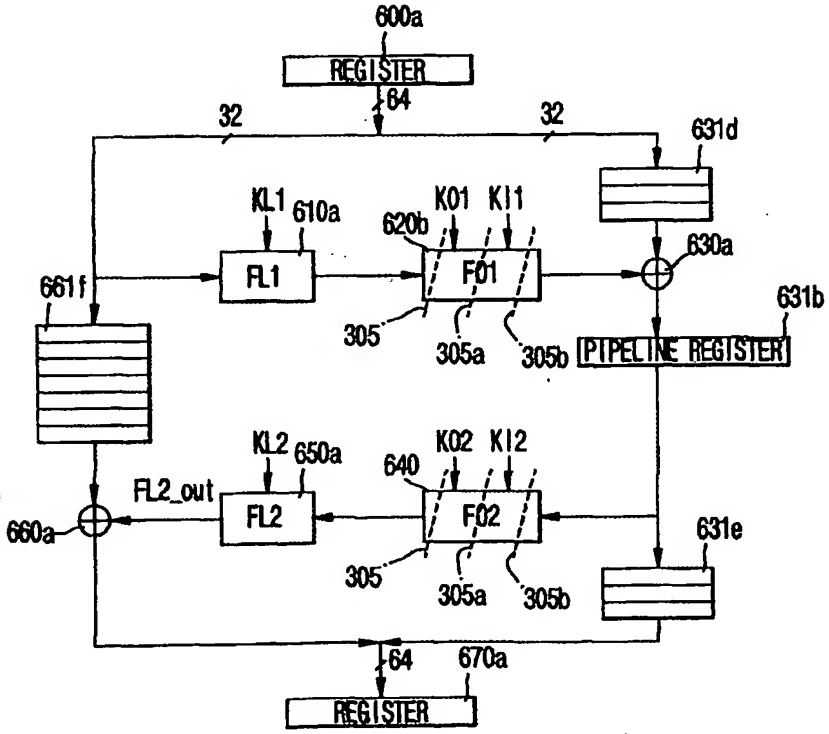

600a
REGISTER
64
32
32
KL1
610a
K01
K11
620a
SYNC REGISTER
631a
FL1
F01
661a
630a
305a
PIPELINE REGISTER
631b
KL2
650a
K02
K12
640a
660a
FL2_out
FL2
F02
305a
SYNC REGISTER
631c
64
670a
REGISTER

FIG.12


600a
REGISTER
64
32
32
631d
KL1
610a
K01
K11
620b
630a
661f
FL1
F01
631b
305
305a
305b
PIPELINE REGISTER
KL2
650a
K02
K12
640
FL2_out
660a
FL2
F02
631e
305
305a
305b
64
670a
REGISTER

INTERNATIONAL SEARCH REPORT

International application No.
PCT/KR02/00695

A. CLASSIFICATION OF SUBJECT MATTER

IPC7 G09C 1/00

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
G09C*, H04L9/06

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched
KR, JP as above

Electronic data base consulted during the intertnational search (name of data base and, where practicable, search terms used)
FPD, USPAT, PAJ, IEL

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
D, A	JP 09269727 A (TOSHIBA Corp) 14 October 1997 See abstract	1, 6
D, A	JP 09251267 A (TOSHIBA Corp) 22 September 1997 See abstract	1, 6
A	US 3962539 A (IBM Corp) 8 June 1976 See the whole document	1, 6

☐ Further documents are listed in the continuation of Box C.

☒ See patent family annex.

* Special categories of cited documents:
"A" document defining the general state of the art which is not considered to be of particular relevence
"E" earlier application or patent but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed
"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevence; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevence; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents,such combination being obvious to a person skilled in the art
"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
29 AUGUST 2002 (29.08.2002)	29 AUGUST 2002 (29.08.2002)

Name and mailing address of the ISA/KR
Korean Intellectual Property Office
920 Dunsan-dong, Seo-gu, Daejeon 302-701,
Republic of Korea
Facsimile No. 82-42-472-7140

Authorized officer
JEONG, Jae Heon
Telephone No. 82-42-481-5672

Form PCT/ISA/210 (second sheet) (July 1998)

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No.
PCT/KR02/00695

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
JP 09269727 A	14-10-1997	NONE	
JP 09251267 A	22-09-1997	NONE	
US 3962539 A	08-06-1976	IT 1055305 A	21-12-1981
		FR 2301873 A	17-09-1976
		CA 1046942 A	23-01-1979
		JP 51108701 A	27-09-1976
		GB 1480858 A	27-07-1977
		DE 2558206 A	09-09-1976